CLAIMS

1. A data processor in which at least one of encryption of a plain text to a cipher text by using an encryption key and decryption of a cipher text to a plain text by using a decryption key is performed, comprising:

a key converting section in which a plurality of key conversion functions which are involution functions, and which conduct key conversions to output extended keys based on one of the encryption key and the decryption key and results of key conversion of one of the encryption key and the decryption key are sequentially connected, and results of the key conversion are in an order or in another order reverse to the order transferred between the key conversion functions; and

a data randomize section in which at least one processing of encryption of the plain text to the cipher text and decryption of the cipher text to the plain text is performed by using the extended keys output from the key conversion section.

2. A data processor according claim 1,

wherein the data randomize section includes a plurality of round functions which are involution functions and which perform at least one of encryption and decryption by using the extended keys, the plurality of round functions are sequentially connected,

and results of the processing by the round functions are transferred in an order or in another order reverse to the order transferred between the plurality of round functions.

3. A data processor according to claim 1,

wherein the key conversion functions not only take first keys and results of conversion of the first keys as objects to be processed in the key conversion, but also perform the key conversion by using a second key.

4. A data processor according to claim 3,

wherein the second key is included in at least one of the encryption key and the decryption key.

5. A data processor according to claim 4,

wherein the second key has different types of keys, at least one of the encryption key and the decryption key includes the different types of keys and at least one of the encryption key and the decryption key is variable in length.

6. A data processor according to claim 2,

wherein the key conversion functions include round functions same as that of the data randomize section.

7. A communication system comprising:

one communication device which includes a data processor according to claim 1 and holds one key which serves as the encryption key and the decryption key; and

another device which includes a data processor according to claim 1 and holds other key which serves as the encryption key and the decryption key, and which is a result of key conversion of the one key in the key conversion section of the another device.

8. A computer readable medium on which a program is recorded, the program being for controlling a data processor in which at least one of encryption of a plain text to a cipher text by using an encryption key and decryption of a cipher text to a plain text is performed by using a decryption key, the program comprising:

a key converting section in which a plurality of key conversion functions, which are an involution function, and which conduct key conversions to output extended keys based on one of the encryption key and the decryption key and results of key conversion of one of the encryption key the decryption key are sequentially connected and results of the key conversion are in an order or in another order reverse to the order transferred between the key conversion functions; and

a data randomize section in which at least one processing of encryption of the plain text to the cipher text and decryption of the cipher text to the plain text is performed by using the extended keys output from the key conversion section.

9. A computer readable medium according to claim 8,

wherein the data randomize section includes a plurality of round functions which are involution functions and which perform at least one of encryption and decryption by using the extended keys, the plurality of round functions are sequentially connected, and results of the processing by the round functions are transferred in an order or in another order reverse to the order transferred between the plurality of round functions.

10. A computer readable medium according to claim 8,

wherein the key conversion functions not only take first keys and results of conversion of the first keys as objects to be processed in the key conversion, but also perform the key conversion by using a second key.

11. A recording medium according to claim 10,

wherein the second key is included in at least one of the encryption key and the decryption key.

12. A recording medium according to claim 11,

wherein the second key has different types of keys, at least one of the encryption key and the decryption key includes the different types of keys and at least one of the encryption key and the decryption key is variable in length.

13. A recording medium according to claim 9,

wherein the key conversion functions include round functions same as that of the data randomize section.

14. A data transformation apparatus comprising:

a key transformation section for outputting a second key and a third key by using an involution function based on inputted first key and for outputting the first key and a fourth key by using the involution function based on inputted second key,

wherein the third key is used when first data is transformed to second data and the fourth key is used when the second data is transformed to the first data.